WHITEPAPER

Cloud security blind spots

(and how to avoid them)

VULCAN.

A new environment means a new attack surface

One of the most underrated and top concerns for companies using cloud services—whether they were born in the cloud or migrated from on-premises—is the security responsibility attached. These concerns stem from the fact that, with so many types of cloud deployment methods and offerings available from cloud service providers (CSPs), security responsibilities can vary greatly depending on the services used.

The most common cloud deployment options include:

- **Public cloud:** involves sharing cloud resources with multiple tenants, and as such is one of the most cost-effective solutions.
- **Private cloud:** offers the advantage of having dedicated resources only for your organization, whether hosted in the organization's on-site data center or the cloud provider's environment.
- **Hybrid cloud:** the combination of a dedicated cloud or on-premises data center with a public cloud.

Common types of cloud offerings include:

- infrastructure as a service (IaaS)
- platform as a service (PaaS)
- software as a service (SaaS)

There are many reasons for cloud security blind spots: poor infrastructure visibility, dark data, misconfigurations, or organizational and management problems. Companies must be fully aware of their security responsibilities, which will depend on the specific cloud offering and deployment used. For example, If a company deploys an EC2 instance from AWS, which is categorized as IaaS, it is responsible for managing and maintaining the operating system, applications hosted in the environment, data and identity, as well as access management (IAM). The cloud provider, in this case, offers only the infrastructure, as seen in Figure 1.

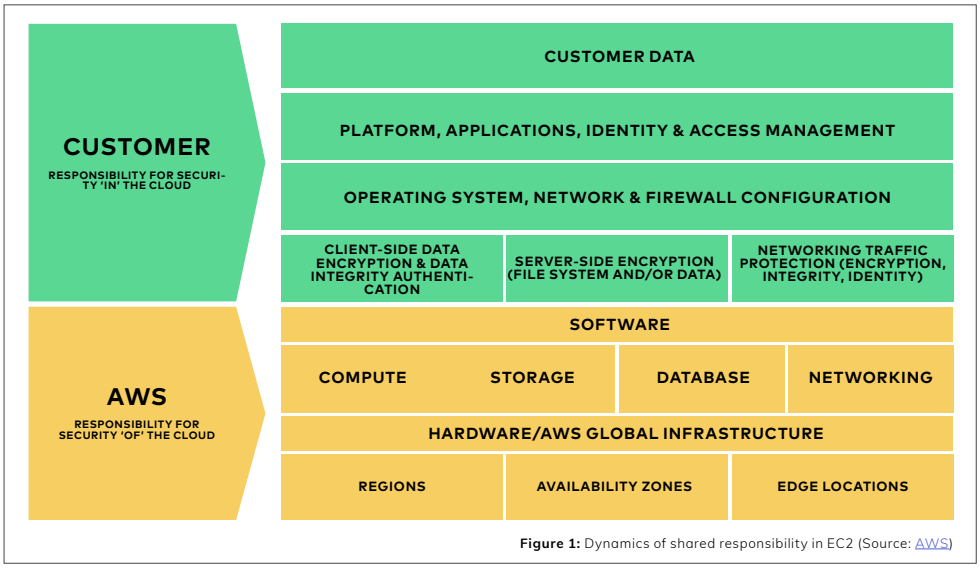


Figure 1: Dynamics of shared responsibility in EC2 (Source: AWS)

But with all these cloud offerings and deployment models to choose from, there are frequently blind spots organizations fail to understand. This white paper covers the common cloud security traps and what you can do to minimize such security issues.

5 cloud security traps

Before choosing a cloud service offering, it is important to be aware of common security traps companies fall into, in order to ensure a seamless experience and reap all the benefits it has to offer.

01

LACK OF AWARENESS ABOUT SECURITY RESPONSIBILITY

While some security controls may be inherited from the cloud provider, the CSP is not responsible for controls such as access management that the client configures on top of the infrastructure the CSP has provided.

Although security of different components (e.g., hardware, virtualization, operating systems, software, etc.) varies depending on the cloud deployment and type, data and IAM always remain the client's responsibility, as shown in Figure 2.

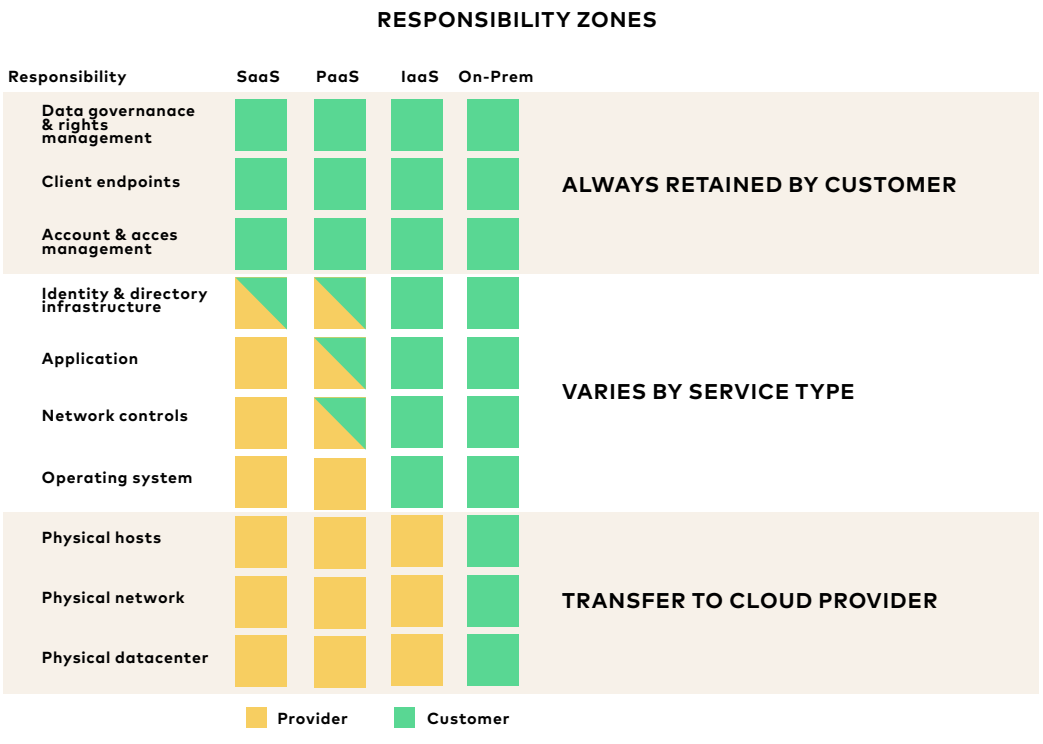


Figure 2: Cloud responsibility zones (Source: AT&T)

It is important that the clients be aware of their CSP's security responsibilities as laid out in their SLA, such as guaranteed availability—a key aspect of security—and security maintenance windows.

But all too often, organizations simply have blind faith in their cloud providers and fail to identify these shifting responsibilities of different offerings and deployments. This can lead organizations to create insecure environments.

02

LACK OF VISIBILITY IN THE ENVIRONMENT

In larger organizations, collaboration among teams does not always happen as flawlessly as it should for many reasons, whether it be due to poorly defined processes, lack of documentation, or other issues. This often leads to access management and identity issues, which can result in situations in which a former employee may have unrestricted access to the environment, for example.

Lack of visibility within the organization's culture thus leads to a blind spot in the cloud environment. And this failure to protect the data in your environment could pose serious risks.

03

COMPLEXITIES IN MULTI-CLOUD SETUPS AND CROSS-FUNCTIONAL TEAMS

Multi-cloud integrations are becoming increasingly popular, as companies look to take advantage of the flexibility to choose the specific services that suit them and that each cloud provider excels in.

Despite the business value the multi-cloud approach brings, it also comes with added complexity. Teams may struggle with cross-functional team collaboration. Vulnerabilities may be detected early on in the development lifecycle by one department, but the fix may need to be completed by a completely different department.

With no proper mechanism to track the findings of the teams, the process may not be properly monitored and important security issues may be overlooked altogether. As companies scale and multi-functional teams work in multi-cloud environments, this can eventually lead to unmanaged resources and dark data. This can result in unidentified risks to the organization, far more alarming than any known risks.

04

DARK DATA

In any organization, the data it holds is one of its most valuable assets. As organizations scale, there may be resources existing in the environment that are not accounted for and identified. This may include projects that were created in the initial stages, testing VMs, or an insecure connection to another environment.

An identified risk is always better so the company is aware of the consequences. Unmanaged dark data, on the other hand, poses a serious risk, as the organization will not have any visibility or be able to evaluate what could go wrong. With no monitoring or alerting set up for the resources where the data resides, a theoretical attack could last for weeks.

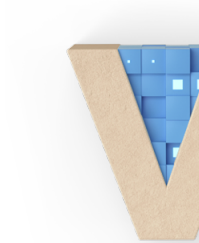
05

ACCESS MANAGEMENT

The principle of least privilege (PoLP) is a general security concept relevant to the cloud as well. Within an organization, employees should only have the necessary access within the framework of their roles and responsibilities. In cases where a person has more access than required, they could perform actions that could cause irreversible damage or that could simply lead to misconfigurations due to a lack of skills. Therefore only those who require it and have the necessary skills should be granted higher access. In all other cases, access should require approval—most critical operations have built-in approval processes to avoid any mistakes.

How to avoid cloud security blind spots

Cloud adoption continues to grow at an impressive pace, but along with technological improvements, the cloud also brings complexities. Cloud security mistakes can happen at both the technical and organizational level. Among organizations working in the cloud, common mistakes include lack of knowledge, uninformed decisions, misconfigurations, and neglecting cloud security responsibilities. Here is how to avoid these.



01 ASSET MANAGEMENT

Because risks are calculated based on assets, proper asset visibility is essential. However, in most large and multi-cloud environments, asset visibility is often minimal in absence of a central platform to manage and monitor this. Architectural complexilities may also result in hidden assets, creating an even larger attack surface due to its unmanaged nature.

---

02 CODE-LEVEL SECURITY CHECKS

As data flows through applications hosted in the environment, code-level security checks can help you understand loopholes and vulnerabilities. These checks help identify application-related security issues before they are released to production. Code changes should not be immediately released to the production environment, and it is important they go through pre-production testing.

Infrastructure as code (IaC) can also help to implement security best practices within the infrastructure along with the use of DevOps tools to avoid network and privilege issues. But IaC should be thoroughly checked to avoid opening ports that are not necessary, insecure configurations, or anything that disables essential security mechanisms.

---

03 PREVENTING DATA LEAKS

Failing to maintain your company's overall security posture could lead to potential data leakages. In the short-term, this could result in financial losses; while long-term consequences may include reputational damage due to lack of trust. Moreover, depending on jurisdiction laws and regulations, this could also result in heavy penalties and SLA breaches with your clients.

To prevent data leaks, IT teams should make sure that systems are hardened according to best practices and provide least privileges. Even with network- and system-level segregation and continuous monitoring, attacks can still happen due to human error. This, however, can be minimized with use of automation tools.

There have been many scenarios where data has been leaked from cloud components such as S3 buckets or databases. And root cause analysis clearly shows that the responsibility does not fall under the CSP's territory. One example to help understand the depth of the problem is the case of Veeam, which in 2018 exposed 445M customer records due to a misconfiguration in MongoDB.

---

04 USE NATIVE CLOUD SECURITY TOOLS

Each of the three main cloud vendors offers vendor-specific security hardening that can be used for system hardening and continuous monitoring. Yet while use of the native cloud tools offered by AWS, Azure, and GCP can certainly minimize blind spots to an extent, they only protect part of the system. Moreover, they don't guarantee security of multi-cloud architectures.

Minimizing cloud security blind spots

Security maturity is the responsibility of all parties involved, but none of these steps can fully eliminate blind spots in your cloud environment. This requires identifying assets that increase the threat landscape and implementing access management policies. In addition, ensuring properly trained personnel, proper management of all technological components, and continuous monitoring can all help reduce your risk.

To this end, a centralized tool can help with continuous monitoring of your cloud environment, discover and address vulnerabilities, and suggest improvements.

Cross-collaboration and prioritizing vulnerabilities are also key, particularly in large organizations where the attack surface is vast. In most organizations, vulnerability detection is the responsibility of the security team, while IT teams are tasked with actually fixing them. Tracking this progress is therefore crucial to ensure efficiency and visibility between teams.

Through automation and remediation playbooks, the Vulcan Cyber® risk management platform streamlines your workflows, keeping your teams updated and on the same page.

With today's demand for cloud services, gaining the competitive edge while still maintaining cyber hygiene and being compliant is key. It is important to identify risks proactively, to prioritize them based on your specific business needs, and to provide risk-based security solutions for cyber risk management.

Infrastructure-level vulnerability management provides limited visibility of your overall security process. The Vulcan Cyber risk management platform covers all your attack surfaces - from cloud and application security to vulnerability management programs - while providing advanced analytics to help you find and prioritize vulnerabilities, even in complex multi-cloud environments. Automation capabilities allow for easy and effective cross-team collaboration, while tracking performance throughout the remediation process.

Ensure your cloud security program is "blind spots free" - own your risk with Vulcan Free.